Consejo de la Unión Europea

Bruselas, 18 de octubre de 2023
(OR. en)

14394/23

COSI 181
CRIMORG 139
ENFOPOL 433
CT 156
COTER 186
AVIATION 194
JAI 1334

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	18 de octubre de 2023
A:	D.ª Thérèse BLANCHET, secretaria general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2023) 659 final
Asunto:	COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO sobre la lucha contra las posibles amenazas que plantean los drones

Adjunto se remite a las delegaciones el documento COM(2023) 659 final.

Adj.: COM(2023) 659 final

COMISIÓN
EUROPEA

Bruselas, 18.10.2023
COM(2023) 659 final

COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO

sobre la lucha contra las posibles amenazas que plantean los drones

I. INTRODUCCIÓN

La presente Comunicación establece la política de la UE para la lucha contra las posibles amenazas de los sistemas de aeronaves no tripuladas (UAS, por sus siglas en inglés) no cooperativos, comúnmente conocidos como «drones». Forma parte de un paquete más amplio de defensa contra los drones que también incluye dos manuales, que ofrecen orientación práctica sobre aspectos técnicos clave de esta política. Este paquete se anunció como una acción emblemática en el marco de la Comunicación de la Comisión «Una Estrategia 2.0 para los drones encaminada a lograr un ecosistema de aeronaves no tripuladas inteligente y sostenible en Europa»[1]. La presente Comunicación responde a la necesidad de: i) proporcionar un marco normativo completo y armonizado, ii) construir un entendimiento común de los procedimientos aplicables para hacer frente a las amenazas en constante evolución que pueden plantear los drones, y iii) tener en cuenta la rápida evolución tecnológica.

A. Completar el marco de la UE sobre los drones

El uso legítimo de drones es un elemento clave del camino hacia la doble transición ecológica y digital, tal como se establece en la «Estrategia 2.0 para los drones» de la UE. Desempeñan una función importante especialmente en los ámbitos del transporte, la defensa, el comercio y los servicios. El número de drones en uso en la UE aumentará significativamente en los próximos años, y estos mejorarán considerablemente en cuanto a su velocidad, agilidad, alcance máximo, capacidades de carga útil, precisión de los sensores y uso de la inteligencia artificial. Estos avances darán lugar a una gama más amplia de usos legítimos y lícitos para los drones. Sin embargo, para que se alcance este potencial, es necesario abordar la amenaza que pueden plantear los drones no cooperativos. Un dron no cooperativo debe definirse en función de la naturaleza de la falta de cooperación, que podría incluir el uso delictivo, ilegal (infracción reglamentaria intencionada) o aficionado (desconocimiento, imprudencia).

La presente Comunicación aborda las amenazas que plantean los drones diseñados para uso civil y pretende hacer frente a las amenazas de estos drones en un entorno civil. Aunque la presente Comunicación no se centra en los drones diseñados para fines de defensa, sigue habiendo diversas interrelaciones con el ámbito de la defensa, entre ellas, el uso potencial de drones más pequeños diseñados con fines de defensa por parte de delincuentes o terroristas, así como las sinergias entre tecnologías para hacer frente a los drones. Los drones diseñados con fines de defensa podrían ocupar el mismo espacio aéreo que los drones civiles y, en estos casos, las autoridades competentes deben poder identificarlos para tener conocimiento de la situación.

El ámbito de aplicación de la presente Comunicación se centra específicamente en *contrarrestar* las posibles amenazas que plantean los drones. Por lo tanto, no pretende abarcar la dimensión más amplia de la función de los drones en el ámbito de la seguridad interior, a saber, su uso para la aplicación de la ley y la seguridad o el orden públicos.

Los Estados miembros son las principales responsables de contrarrestar las amenazas que plantean los drones no cooperativos. Sin embargo, los Estados miembros también se benefician de la actuación a escala de la UE, que permite una cooperación y una coordinación más estrechas en los diferentes medios e instrumentos utilizados a tal efecto. Por lo tanto, la presente Comunicación promueve diferentes medidas

[1] Una Estrategia 2.0 para los drones encaminada a lograr un ecosistema de aeronaves no tripuladas inteligente y sostenible en Europa, COM(2022) 652 final, de 29 de noviembre de 2022.

relacionadas con la creación de comunidades y el intercambio de información. También apoya a los Estados miembros con orientación, formación, financiación y procedimientos operativos.

Los incidentes potencialmente peligrosos relacionados con drones se han vuelto más frecuentes, tanto dentro de la UE como fuera de sus fronteras. Por lo tanto, es importante facilitar la adopción de soluciones físicas o digitales de defensa contra los drones por parte de las autoridades policiales y otras autoridades públicas de la UE y de los operadores de infraestructuras críticas. La elaboración de una política de la UE para la defensa contra los drones contribuirá a reforzar los procedimientos de prueba de la eficiencia de las nuevas soluciones disponibles y a facilitar el uso específico de la investigación y la innovación en este ámbito. Con la elaboración de esta política para la defensa contra los drones, la Comisión contribuye a reforzar un mercado de la UE de soluciones en este ámbito. Esto allanará el camino para una mayor autonomía estratégica y soberanía tecnológica de la UE, en particular en los ámbitos de tecnologías críticas. Fomentará las capacidades europeas para desarrollar soluciones de vanguardia en los ámbitos de la defensa, el sector aeroespacial y la seguridad civil y reducirá la dependencia de proveedores no europeos. Se basará en los resultados de la evaluación de las dependencias tecnológicas críticas[2] y proporcionará más datos y análisis. Además: i) aportará información a la percepción de la Comisión sobre el uso de tecnologías críticas y la dependencia de proveedores no europeos, y ii) ofrecerá una sólida visión general del nivel de dependencia.

Además, con el fin de hacer frente a las amenazas que plantean los drones no cooperativos desde el punto de vista de las autoridades públicas, también es importante: i) disponer de marcos y procedimientos claros y armonizados, ii) ofrecer competencias claras al as partes interesadas públicas y privadas responsables para intervenir contra los drones no cooperativos, y iii) facilitar la colaboración entre las partes interesadas que no siempre están acostumbradas a trabajar juntas (fuerzas y cuerpos de seguridad, autoridades de aviación civil, operadores, fabricantes u operadores de redes móviles). La presente Comunicación propone medidas para: i) construir un entendimiento común de los procedimientos aplicables a la hora de hacer frente a las amenazas que plantean los drones, e ii) identificar posibles necesidades en términos de armonización de las medidas reglamentarias.

B. Abordar una amenaza actual y en rápida evolución

Tanto la estrategia de la UE para una «Unión de la Seguridad»[3] como la Agenda de Lucha contra el Terrorismo[4] subrayan que la amenaza de los drones no cooperativos es motivo de gran preocupación en Europa.

El rápido avance de las capacidades de los drones plantea un riesgo cada vez mayor para la seguridad. En los últimos años se han descubierto planes para intentar utilizar drones en atentados terroristas[5]. También se han avistado drones sospechosos en torno a infraestructuras críticas, como instalaciones de energía, aeropuertos y puertos, lo que indica el posible uso indebido de drones para la recopilación hostil de información. Los drones son utilizados por delincuentes implicados en el contrabando transfronterizo o

[2] En 2022, se llevó a cabo una evaluación interna detallada de la Comisión sobre los sistemas autónomos.

[3] Estrategia de la UE para una Unión de la Seguridad, COM(2020) 605, de 24 de julio de 2020.

[4] Agenda de lucha contra el terrorismo de la UE: anticipar, prevenir, proteger, responder», COM(2020) 795 final, de 9 de diciembre de 2020.

[5] Cabe citar a modo de ejemplo: i) el plan de un yihadista que fue condenado por un tribunal español en octubre de 2022 por planear atacar un estadio con un dron cargado con explosivos durante un partido de fútbol importante, y ii) un ciudadano belga, condenado por tentativa de atentado con bomba utilizando drones contra una prisión.

para facilitar otras operaciones ilícitas, como el tráfico de drogas. Además, los drones pueden ser una fuente de riesgos cibernéticos, por ejemplo, si se utilizan para el reconocimiento digital. Las amenazas que plantean los drones no son simplemente un problema técnico. Hoy en día, la mayoría de los drones diseñados con fines civiles pueden ser detectados e identificados, pero sigue siendo muy difícil controlarlos o neutralizarlos (es decir, tomar el control del dron, hacerlo aterrizar de forma segura o derribarlo), a menudo debido a la falta de autorización judicial para hacerlo. Esto es particularmente cierto por lo que respecta a operadores privados de infraestructuras críticas. Por lo tanto, la lucha contra las amenazas que plantean los drones debe tenerse en cuenta en futuras evaluaciones de riesgos con arreglo a la Directiva relativa a la resiliencia de las entidades críticas[6].

El panorama de las amenazas se percibe aún más claro si se consideran los incidentes en países cercanos a la UE y en otras partes del mundo. Se ha constatado que los drones son una plataforma de doble uso rentable y eficaz que ha impulsado la innovación en materia de defensa en la guerra rusa contra Ucrania. El uso de drones diseñados con fines civiles para ataques destructivos incluso en otros conflictos armados (como en Yemen o Siria) es un fenómeno que puede tener implicaciones directas para la seguridad interior de la UE. El *modus operandi* de los grupos terroristas y la mejora de las capacidades en el uso de «drones disponibles en el mercado» podrían llegar a nuestras fronteras y representar una amenaza. Lo mismo ocurre con el uso de drones para intentos de asesinato selectivos[7].

Sin embargo, las soluciones para la defensa contra los drones no solo son necesarias para hacer frente a los usos malintencionados selectivos, sino también para evitar incidentes provocados por negligencia o imprudencia. La mayoría de los usuarios de drones en la UE (en particular, los pilotos profesionales a distancia con licencia o los pilotos de ocio organizado) cumplen las normas, reglamentos y limitaciones técnicas existentes. No obstante, los usuarios de drones que hacen uso de estos con desconocimiento, imprudencia y para delinquir, son responsables de los numerosos incidentes peligrosos relacionados con los drones que se producen en toda la UE. Los acontecimientos públicos a gran escala son especialmente vulnerables a tales perturbaciones, al igual que algunos sectores críticos como el transporte aéreo. Además, el uso ilícito de drones también puede afectar a la seguridad personal y al derecho a la intimidad de la ciudadanía, en particular cuando los drones se utilizan en zonas residenciales.

C. Seguir el ritmo de los avances tecnológicos

La protección de nuestras sociedades de los drones malintencionados y no cooperativos requiere el acceso a medidas de respuesta asequibles y fiables que permitan soluciones flexibles. Las soluciones suelen abordar tres aspectos: la detección, el seguimiento y la identificación. Además de estos, las autoridades públicas están interesadas en dos aspectos adicionales: la neutralización y la criminalística.

Tanto en el ámbito de la defensa como en el de la seguridad civil, ya se están desarrollando y probando soluciones innovadoras para la defensa contra los drones. Su entrada en el mercado y su adopción por parte de los usuarios finales pueden facilitarse mediante un marco general de la UE para luchar contra los drones, tal como se promueve en la presente Comunicación. Sin embargo, no es posible adoptar un enfoque único normalizado para la aplicación de medidas de defensa contra los drones debido a la gran variedad de posibles escenarios y entornos operativos.

---

[6] Directiva (UE) 2022/2557, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas (DO L 333 de 27.12.2022, p. 164).

[7] Cabe citar a modo de ejemplo el intento infructuoso de asesinar al presidente de Venezuela y el uso de drones por parte de los cárteles mexicanos de la droga contra representantes de otras organizaciones delictivas.

Por lo tanto, las medidas de defensa contra los drones deben adaptarse a las diferentes necesidades y entornos operativos. Desde el punto de vista de las autoridades encargadas de la seguridad interior, puede haber situaciones en las que la destrucción física total de un dron sea la opción preferida y única, por ejemplo, para evitar un ataque inminente contra personas o infraestructuras. En otros casos, como el uso delictivo o la recopilación hostil de información, existe un gran interés en garantizar el control del dron para hacer que este aterrice, dejándolo lo más intacto posible, para posibilitar una investigación forense óptima. Esto incluye la necesidad de soluciones cibernéticas sofisticadas para tomar el control del sistema operativo de los drones.

Una de las tendencias tecnológicas que deben supervisarse y utilizarse activamente es el desarrollo de sensores para una detección más precisa de los drones. Las capacidades de los sensores existentes pueden seguir desarrollándose no solo para detectar un dron, sino también para evaluar la amenaza que supone mediante el análisis de patrones de vuelo, la detección de la carga útil y la detección de equipos. Los sensores y los sistemas de detección deben ser capaces de hacer frente a las cambiantes formas y capacidades de los drones (velocidad, agilidad, capacidad de desplegar señuelos, etc.). La capacidad de las autoridades públicas y los operadores privados de infraestructuras críticas para analizar los datos procedentes de estos sensores será cada vez más importante. La inteligencia artificial también desempeñará un papel en ello, por ejemplo, mediante la generación automática de alertas, el cálculo de riesgos, la predicción de rutas o la previsión de lugares de aterrizaje. Así, las nuevas tendencias en los mercados de drones deben ser objeto de un seguimiento continuo e incorporarse a las soluciones de defensa contra los drones. El seguimiento de estos avances tecnológicos debe permitir a las autoridades de la UE determinar las prioridades de inversión y apoyar aquellos avances que mejor se adapten a las necesidades operativas expresadas por las autoridades policiales y los operadores privados de los Estados miembros.

En cuanto a la interacción y la neutralización, es necesario seguir probando tecnologías adecuadas en diferentes entornos y escenarios. En el ámbito de la defensa, se han hallado soluciones para destruir físicamente o capturar completamente un dron mientras está en el aire, reduciendo así la generación de residuos que podrían causar lesiones a personas o daños a objetos. Esto incluye la energía dirigida en forma de láseres de alta energía, el uso de sistemas de radiofrecuencia y captura neta de gran potencia, así como herramientas digitales para lograr el control de drones no cooperativos.

Para la aplicación de la ley y la investigación, sería especialmente útil poder neutralizar una amenaza de drones tomando el control de su sistema de control y forzando su aterrizaje de forma segura, lo que daría a las autoridades e investigadores el mejor acceso posible a potenciales pruebas físicas y digitales. Por lo tanto, es necesario contar con una amplia gama de soluciones disponibles y validadas para diferentes fines para servir al ámbito de la seguridad interior. Es por ello necesario fomentar un auténtico mercado y entorno de innovación para soluciones de defensa contra los drones que respondan a las necesidades del ámbito de la seguridad civil. De lo contrario, es poco probable que la evolución de las soluciones de defensa contra los drones siga el ritmo en constante aumento del número y las capacidades de los propios drones. También es esencial estructurar y segmentar este mercado para ayudar a las autoridades correspondientes a identificar las soluciones que mejor respondan a sus necesidades.

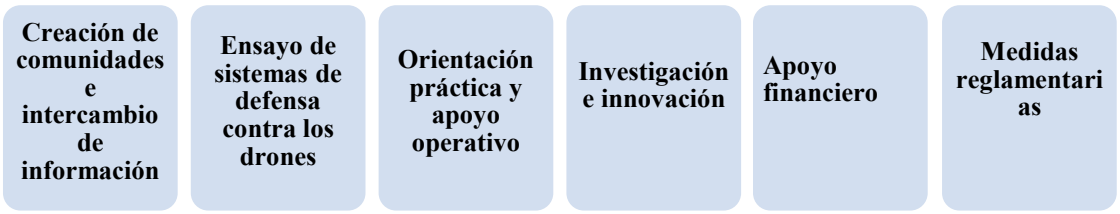
Además, es importante supervisar los sistemas utilizados por los delincuentes para contrarrestar las medidas de defensa contra los drones. Estos sistemas son dispositivos que transporta el dron o que se despliegan desde el suelo y están diseñados para impedir las medidas específicas contra los drones.

Por último, muchos sistemas de defensa contra los drones también se desarrollan con fines de defensa. Aunque difieren en cuanto a los requisitos, a menudo comparten características y tecnologías comunes con sistemas destinados a fines civiles, lo que hace necesaria una estrecha cooperación con el ámbito de la defensa.

Este panorama tecnológico en evolución también requiere un marco regulador coherente y continuamente actualizado para el uso de sistemas de defensa contra los drones.

II. FORMULAR UNA POLÍTICA DE LA UE PARA LA DEFENSA CONTRA LOS DRONES

La Comisión ha colaborado con los Estados miembros y otras partes interesadas sobre la posible amenaza que representan los drones desde 2016, cuando tuvo lugar el primer taller de la UE de defensa contra los drones. Desde entonces, se han propuesto una amplia gama de iniciativas para facilitar la creación de comunidades, el intercambio de información, el desarrollo de mejores prácticas y la financiación específica de proyectos. Como resultado de las conversaciones con expertos de los Estados miembros, la Comisión seguirá apoyando las iniciativas en curso y desarrollando e integrando nuevas líneas de trabajo para elaborar una verdadera política de la UE para la defensa contra los drones. Este trabajo consistirá en las seis actividades clave siguientes:



A. Creación de comunidades e intercambio de información

En la actualidad, una gran variedad de redes y agentes diferentes trabajan a escala de la UE en soluciones para la defensa contra los drones. Por lo tanto, es necesario racionalizar y orientar sus futuras actividades en términos políticos, técnicos y operativos para: i) crear comunidades de partes interesadas que funcionen correctamente, ii) garantizar el intercambio efectivo de información y mejores prácticas, y iii) evitar la duplicación del trabajo.

La Comisión fomentará las iniciativas existentes a nivel técnico, a la vez que creará un **grupo de expertos de la Comisión para la defensa contra los drones** que asesorará en el ámbito de las políticas. Este grupo de expertos podrá hacer aportaciones estratégicas a diversas políticas a escala de la UE pertinentes para las actividades de defensa contra los drones, por ejemplo, en los ámbitos de la seguridad interior, la gestión de fronteras o la resiliencia de las infraestructuras críticas. A tal fin, el grupo de expertos cooperará con otros grupos de expertos y, cuando proceda, con los grupos de trabajo pertinentes del Consejo.

Además, se celebran periódicamente talleres y reuniones de expertos sobre soluciones y políticas de defensa contra los drones. Estos reúnen a responsables políticos, expertos técnicos e investigadores de la Comisión, Estados miembros, otras instituciones de la UE, agencias de la UE, proyectos financiados por la UE, organizaciones internacionales y países socios. Estas actividades han dado lugar a la participación continua de todas las partes interesadas, facilitando significativamente su cooperación operativa y práctica. Con este fin, la Comisión ha creado el **Counter-UAS Information Hub [Centro de información de defensa contra los UAS]**[8], que cuenta actualmente con más de 300 miembros. Esta plataforma en línea se actualiza periódicamente e incluye diferentes fuentes de información, como los resultados de proyectos relevantes financiados por la UE, presentaciones, informes y un boletín semestral.

Otra parte importante de la creación de comunidades y el intercambio de información, en particular para las necesidades operativas de las fuerzas y cuerpos de seguridad, se lleva a cabo como parte de las **redes policiales europeas** financiadas por la UE. Por ejemplo, las siguientes redes han iniciado sus propias actividades para hacer frente a las amenazas que plantean los drones: la Red Europea de Servicios Tecnológicos Policiales (ENLETS, por sus siglas en inglés); la Red Europea de Servicios de Policía Aeroportuarios (AIRPOL); la Red de Unidades Especiales de Intervención de la UE (ATLAS); y la Red de seguridad de alto riesgo de la UE. El recién creado Grupo de trabajo de la red policial, una iniciativa de la Dirección General de Migración y Asuntos de Interior (DG HOME) destinada a fomentar la cooperación entre las redes policiales y financiada por la Comisión[9], racionalizará las líneas de trabajo en curso en el ámbito de la defensa contra los drones en un subgrupo de trabajo específico.

La **Agencia Europea de Seguridad Aérea (AESA)** ha elaborado directrices no vinculantes para ayudar a las autoridades y los aeropuertos a prepararse, responder y recuperarse de los incidentes con drones[10]. Con el fin de promover actividades de apoyo fundamentadas y elaboración de políticas a escala de la UE, es esencial mantener intercambios de información fiables y detallados sobre incidentes relacionados con drones en la UE más allá de los intercambios que ya tienen lugar en zonas críticas específicas, como los

---

[8] Mediante la plataforma CIRCABC de la UE, apoyada por el programa ISA² de la Comisión Europea, que promueve soluciones de interoperabilidad para las administraciones públicas europeas.

[9] El Grupo de Trabajo (informal) de la red policial (LENWG, por sus siglas en inglés) está presidido por la Comisión y se reunió por primera vez el 20 de marzo de 2023 para promover una mejor cooperación entre las redes financiadas por la DG HOME. Tras un período de evaluación de doce meses, el LENWG podría convertirse en un grupo de expertos de la Comisión.

[10] La Agencia Europea de Seguridad Aérea (AESA) publicó en marzo de 2021 un conjunto de directrices para la gestión de incidentes con drones en los aeropuertos: *Drone Incident Management at Aerodromes* [«Gestión de incidentes con drones en aeródromos», documento en inglés].

aeropuertos. De este modo y respetando plenamente la confidencialidad de las investigaciones, existe un potencial significativo para mejorar el intercambio de información sobre: i) los métodos utilizados por los operadores de drones no cooperativos, ii) los patrones de amenaza específicos, y iii) los riesgos potenciales detectados. A fin de facilitar y armonizar el intercambio de la información sobre incidentes, la Comisión compartió con los Estados miembros una plantilla para la notificación de incidentes con drones. Para seguir mejorando la calidad y la frecuencia del intercambio de información, la Comisión estudiará la posibilidad de crear una **plataforma digital que contenga información sobre incidentes con drones** para su uso por las autoridades públicas pertinentes. La plataforma podría servir para identificar y cotejar adecuadamente los principales incidentes de seguridad en los que intervienen drones en la UE. Esta podría incluir también la dimensión cibernética, ya que los drones se utilizan no solo para el reconocimiento visual, sino también para el reconocimiento digital. La plataforma sería coherente con las obligaciones de notificación recogidas en el Reglamento (UE) n.º 376/2014[11] y no duplicaría los esfuerzos existentes.

La Comisión también organizará periódicamente reuniones confidenciales para promover el intercambio de la experiencia adquirida de los incidentes en un formato adecuado.

Medidas clave para la creación de comunidades y el intercambio de información

- **La Comisión creará un grupo de expertos, compuesto por expertos de los Estados miembros y otras partes interesadas, sobre las actividades de defensa contra los drones.**
- **La Comisión estudiará la posibilidad de desarrollar una plataforma digital que contenga información sobre incidentes con drones.**
- **La Comisión organizará reuniones periódicas para facilitar el intercambio de información confidencial entre los Estados miembros sobre incidentes graves de seguridad que impliquen el uso de drones.**

B. Ensayo de los sistemas de defensa contra los drones: identificación y puesta a prueba de soluciones

Los Estados miembros y las autoridades locales pueden elegir entre una gran variedad de soluciones comerciales para la defensa contra los drones, cibernéticas y no cibernéticas, disponibles en el mercado. La elección es difícil, especialmente para las entidades locales que no disponen de capacidades técnicas suficientes. La Comisión ayudará a las autoridades de los Estados miembros a elegir correctamente según sus necesidades operativas, proporcionando asesoramiento y orientación a través del grupo de expertos específico de defensa contra los drones y del trabajo del Centro Común de Investigación (JRC, por sus siglas en inglés) de la Comisión.

En 2019, se pusieron en marcha actividades a escala de la UE para probar los sistemas de defensa contra los drones. Su objetivo es desarrollar una metodología común para evaluar los sistemas que pueden utilizar las autoridades policiales y otras autoridades públicas para detectar, rastrear e identificar drones potencialmente malintencionados. Un pilar central de estas actividades es el proyecto «Courageous»[12] (2021-2024), financiado por el Fondo de Seguridad Interior-Policía (FSI-Policía). Este proyecto está dirigido por la Real Academia Militar de Bélgica y se le han encomendado las siguientes tareas: i) la

[11] Reglamento (UE) 376/2014 del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativo a la notificación de sucesos en la aviación civil.

[12] https://courageous-isf.eu/.

identificación de escenarios estándar adecuados para el ensayo de los sistemas de defensa contra los drones, ii) el desarrollo de requisitos funcionales y de rendimiento, y iii) el desarrollo de una metodología de ensayo. El proyecto también está probando el rendimiento de los sensores y los sistemas integrados. Los resultados del proyecto se comparten continuamente con los Estados miembros, así como con determinados países socios y organizaciones internacionales. Una vez finalizado el proyecto, la Comisión y el consorcio «Courageous» presentarán opciones a los Estados miembros para garantizar la sostenibilidad del proyecto y recomendarán una **metodología para las instalaciones de ensayo de sistemas de defensa contra los drones** en los Estados miembros.

Los avances tecnológicos pertinentes para los sistemas de defensa contra los drones evolucionan rápidamente. Por ello, las actividades de ensayo deben completarse con un seguimiento constante de las tendencias para identificar tanto las soluciones más prometedoras como cualquier posible nuevo reto para el desarrollo de sistemas de defensa contra los drones. El JRC ha aumentado su capacidad para llevar a cabo este seguimiento e identificar estos nuevos retos, lo que beneficia a los Estados miembros y aporta una valiosa contribución a las iniciativas de ensayo a escala de la UE. La información se compartirá a través de los canales adecuados, en particular el grupo de expertos.

La normalización es un instrumento para armonizar las soluciones tecnológicas. El proyecto «Courageous» elaboró un asesoramiento específico sobre prenormalización, a partir del cual puede evaluarse más a fondo la viabilidad y la necesidad de poner en marcha procesos de normalización. A escala de la UE, se ha avanzado mucho en el desarrollo de requisitos voluntarios de rendimiento para los equipos de detección fuera de la aviación (por ejemplo, para las máquinas de rayos X y los detectores de metales[13]). Junto con expertos de los Estados miembros y de la industria, la Comisión también desarrollará a continuación **requisitos voluntarios de rendimiento** cuando proceda de manera coherente con las disposiciones del Reglamento sobre la Ciberseguridad[14]. El establecimiento de un proceso de certificación de los sistemas de defensa contra los drones debe seguir siendo un objetivo a medio plazo. Cuando proceda, también se tendrán en cuenta las normas híbridas de protección civil.

Otro elemento clave es normalizar y certificar la ciberseguridad de los sistemas de defensa contra los drones, especialmente si son suministrados por proveedores de terceros países. En esta fase, persiste la incertidumbre sobre el grado de protección de los datos recopilados por determinados sistemas de detección. Además, es importante evitar en la medida de lo posible el pirateo y el uso indebido de los sistemas de defensa contra los drones garantizando la ciberresiliencia de sus componentes.

En septiembre de 2022, la Comisión adoptó una propuesta de Reglamento sobre ciberresiliencia[15], cuyo objetivo es elaborar normas generales de ciberseguridad para los productos con componentes digitales (tanto *hardware* como *software*) que accedan al mercado único. El nuevo Reglamento propuesto tiene por objeto introducir requisitos de ciberseguridad obligatorios para estos productos. Estos requisitos incluirán la ciberseguridad desde el diseño y por defecto, así como requisitos para abordar la vulnerabilidad. Tal como propone la Comisión, los sistemas de drones que no se desarrollen exclusivamente con fines militares o de seguridad nacional y que no estén ya certificados de conformidad con el Reglamento (UE) 2018/1139

[13] Recomendación de la Comisión relativa a los requisitos voluntarios de rendimiento de los equipos de rayos X utilizados en los espacios públicos, C(2022) 4179 final.

[14] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación.

[15] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020, COM(2022) 454 final.

estarían cubiertos como productos con elementos digitales por estas nuevas normas, a excepción de los desarrollados exclusivamente con fines de seguridad nacional o defensa.

Medidas clave para el ensayo de los sistemas de defensa contra los drones

- **La Comisión trabajará en la aplicación de una metodología de ensayo armonizada para los sistemas de defensa contra los drones basada en los resultados del proyecto «Courageous».**
- **El JRC elaborará un informe anual sobre la evolución técnica de la tecnología de defensa contra los drones.**
- **La Comisión, en cooperación con los correspondientes grupos de expertos, como las redes policiales ENLETS, HRSN y AIRPOL, desarrollará un conjunto de requisitos voluntarios de rendimiento para los sistemas de defensa contra los drones.**

C. Orientación práctica y apoyo operativo

La lucha contra las amenazas que plantean los drones no cooperativos ya ha sido identificada como una prioridad en una serie de publicaciones del JRC, por ejemplo, en directrices centradas en la construcción de una protección perimetral[16] y en el estudio específico sobre las cargas explosivas[17] transportadas por drones. Además, la reciente publicación[18] sobre el concepto de seguridad desde el diseño pone de relieve la importancia de integrar medidas de protección proporcionadas, adecuadas y multifuncionales en un enfoque bien elaborado desde el inicio de la fase de planificación y diseño de un proyecto, incluidas medidas para contrarrestar cualquier ataque que haga uso de drones.

Además, el manual de la AESA *Drone Incident Management at Aerodromes* [«Gestión de incidentes con drones en aeródromos», documento en inglés] ofrece orientaciones sobre cómo desarrollar mecanismos y procedimientos adecuados que apoyen un sistema de respuesta a incidentes en los aeropuertos que sea rápido, eficaz y proporcionado. De este modo, las suspensiones del tráfico aéreo o el cierre del espacio aéreo o de las pistas, pueden evitarse o reducirse al mínimo y los cierres de aeropuertos seguirían siendo el último recurso. El trabajo de la AESA tiene en cuenta las orientaciones de la Organización de Aviación Civil Internacional sobre la seguridad aérea[19].

El JRC ha elaborado dos manuales nuevos:

- ***Protection against Unmanned Aircraft Systems:*** *Handbook on UAS protection of Critical Infrastructure and Public Space - A five Phase approach for C-UAS stakeholders* [«Protección contra los sistemas de aeronaves no tripuladas. Manual sobre la protección frente a los UAS de las infraestructuras críticas y el espacio público: Enfoque en cinco fases para las partes interesadas de los C-UAS», documento en inglés].

---

[16] Karlos, V. y Larcher, M., Guideline, *Building Perimeter Protection* [«Construir una protección perimetral», documento en inglés], EUR 30346 EN, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2020.

[17] La amenaza de los UAS que utilizan explosivos fue investigada por el JRC en: Larcher M, Karlos V, Valsamos G, Solomos G: *Scenario study: drones carrying explosives* [«Estudio de situación, drones que transportan explosivos», documento en inglés], JRC107683, 2018.

[18] Comisión Europea, *Security by Design: Protection of public spaces from terrorist attacks* [«Seguridad desde el diseño: protección de los espacios públicos de ataques terroristas», documento en inglés], JRC131172, 2022.

[19] El *Aviation Security Manual* de la OACI (Doc 8973 – Restricted) [«Manual de seguridad de la aviación», documento en inglés] ayuda a los Estados miembros a aplicar el anexo 17 del Convenio de Chicago proporcionando orientaciones sobre cómo aplicar sus normas y prácticas recomendadas (SARPs, por sus siglas en inglés).

- ***Protection against Unmanned Aircraft Systems:*** *Handbook on UAS Risk Assessment and Principles for Physical Hardening of Buildings and Sites.*

En el ámbito de la **formación**, el proyecto DroneWISE[20], financiado por la UE, creó un paquete de estrategias de mando, control y coordinación de la defensa contra los drones para los primeros intervinientes. El proyecto también elaboró diez módulos de formación, un manual y un portal de formación en línea. Estos módulos de formación se han integrado en el plan de estudios de la CEPOL, la Agencia de la Unión Europea para la Formación Policial. Otro de los proyectos del FSI dedicado a la formación para la defensa contra los drones fue el proyecto Skyfall. Es necesario hacer llegar la formación disponible a los proveedores de seguridad privada, en particular a los responsables de la protección de las infraestructuras críticas.

El **programa de asesores de seguridad de la UE**[21] de la Comisión cuenta con una sección dedicada a las actividades de defensa contra los drones, que ofrece: i) una evaluación específica de la vulnerabilidad de las instalaciones e infraestructuras de alto riesgo, ii) consejos prácticos sobre cómo hacer frente a la amenaza de los drones, y iii) consejos prácticos sobre cómo hacer frente al despliegue de equipos de detección de drones durante eventos de alto riesgo. La Comisión estudiará la necesidad de crear una reserva de la UE de los equipos de defensa contra los drones a disposición de los Estados miembros a fin de apoyar estos en eventos a gran escala.

Los **ejercicios** como los organizados con la red policial a escala de la UE contribuyen a la preparación operativa en diferentes ámbitos de la seguridad interior. Cuando proceda, la Comisión trabajará con las redes pertinentes para incluir elementos de defensa contra los drones en ejercicios futuros. Esto contribuirá a seguir aumentando el conocimiento y el intercambio de mejores prácticas, utilizando diferentes soluciones. Uno de los requisitos para responder eficazmente a las amenazas que plantean los drones es la comunicación segura y fiable entre las distintas autoridades. Por lo tanto, la lucha contra las amenazas que plantean los drones formará parte de la planificación del futuro ejercicio que se llevará a cabo en el marco del proyecto de preparación de BroadEU.Net financiado por la UE, poniendo a prueba la base del futuro sistema de comunicación crítica de la UE[22]. Además, podrían llevarse a cabo ejercicios conjuntos que incluyan a expertos en ciberseguridad y seguridad de drones que aborden los riesgos cibernéticos que plantean los drones, así como soluciones digitales para neutralizarlos.

Acciones clave para la orientación práctica y el apoyo operativo

- **El JRC publicará dos manuales como parte del paquete de defensa contra los drones.**
- **La Comisión, en cooperación con las agencias pertinentes, apoyará la ampliación de la formación existente en materia de defensa contra los drones al sector de la seguridad privada.**
- **La Comisión integrará los componentes de la defensa contra los drones en la planificación de ejercicios, en cooperación con las redes policiales.**

[20] https://dronewise-project.eu/.

[21] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en.

[22] El sistema de comunicación crítica de la UE proporcionará una infraestructura segura y de banda ancha para garantizar la interoperabilidad transfronteriza de los sistemas de comunicación utilizados por las fuerzas y cuerpos de seguridad y los servicios de emergencia en el espacio Schengen.

D. Investigación e innovación

La UE sigue financiando su programa de investigación en materia de seguridad como parte de**Horizonte Europa (2021-2027)**[23]. Este programa de investigación en materia de seguridad representa aproximadamente el 50 % de la financiación pública total invertida en la UE y sus Estados miembros en el ámbito de la seguridad. Como contribuyente estratégica a diversas prioridades de la política de seguridad de la UE, esta investigación en materia de seguridad también ha empezado a abordar las amenazas que plantean los drones. Algunos ejemplos destacados son ALADDIN, que ofrece soluciones para detectar y neutralizar drones en zonas restringidas[24], o 7SHIELD, que investigó el desarrollo de soluciones de defensa contra los drones para segmentos terrestres de infraestructuras espaciales críticas. El proyecto ALFA también logró desarrollar un sistema para detectar y rastrear drones utilizados para el contrabando[25]. Estas iniciativas de investigación e innovación podrían continuar en el marco de Horizonte Europa, validadas o complementadas por acciones emprendidas en el marco del FSI-Policía.

En el futuro, la Comisión facilitará un intercambio más sistemático de los resultados de proyectos importantes con las partes interesadas pertinentes, también a través de la Comunidad Europea de Investigación e Innovación en materia de Seguridad[26], lo que podría reforzar aún más el intercambio de datos específicos. También permitiría aunar de manera más eficiente las necesidades de los usuarios y comunicarlas a la industria con el fin de orientar la innovación. Además, el intercambio sistemático de los resultados de los proyectos contribuirá a hacer posible un diálogo estructurado con los Estados miembros y las partes interesadas para identificar tecnologías, herramientas y soluciones prometedoras que podrían ser adoptadas por un grupo de autoridades de los Estados miembros. En este contexto, la Comisión evaluará con los Estados miembros[27] la posibilidad de: i) crear un tema de investigación independiente sobre soluciones de defensa contra los drones en los futuros programas de trabajo de Horizonte Europa, y ii) apoyar sistemas innovadores específicos a través de la contratación precomercial[28]. Esto está plenamente en consonancia con el enfoque orientado a las capacidades que se detalla en el documento de trabajo de los servicios de la Comisión sobre la mejora de la seguridad mediante la investigación y la innovación[29].

Es fundamental reforzar las sinergias en las soluciones de defensa contra los drones entre las industrias europeas de seguridad civil, defensa y espacio. El objetivo debe ser fomentar las sinergias en las tecnologías

[23] Anteriormente, hasta finales de 2020, la investigación y la innovación en materia de seguridad se financiaban en el marco de Horizonte 2020 y del Séptimo Programa Marco.

[24] https://cordis.europa.eu/project/id/740859.

[25] ALFA es también la base del proyecto «Courageous» del FSI y sus actividades de ensayo.

[26] La Comunidad Europea de Investigación e Innovación en materia de Seguridad (CERIS por sus siglas en inglés) reúne a partes interesadas de la investigación en seguridad, desde los responsables políticos, los usuarios finales, el mundo académico y la industria hasta la seguridad civil: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_es.

[27] En la configuración del comité del programa Horizonte Europa «Seguridad civil para la sociedad».

[28] La contratación precomercial es un enfoque de la contratación pública de servicios de investigación y desarrollo (I+D) que se esbozó en la Comunicación sobre la contratación precomercial [C(2007) 799 final] de 14 de diciembre de 2007. Se trata de una herramienta importante para estimular la innovación, ya que permite al sector público orientar el desarrollo de nuevas soluciones hacia sus necesidades.

[29] Documento de trabajo de los servicios de la Comisión *Enhancing security through research and innovation* [«Mejorar la seguridad mediante la investigación y la innovación», documento en inglés], SWD(2021) 422 final de 15 de diciembre de 2021.

de drones y de defensa contra los drones entre los tres sectores[30]. En la práctica, el refuerzo de estas sinergias significa que los proyectos de defensa pueden beneficiarse de avances innovadores en el ámbito civil, mientras que la aeronáutica civil puede beneficiarse de los avances en la defensa.

El **Fondo Europeo de Defensa (FED)** y sus programas precursores incentivan y apoyan la investigación y el desarrollo colaborativos y transfronterizos en el ámbito de la defensa. Como complemento y ampliación de los esfuerzos de los Estados miembros, el FED promueve la cooperación entre empresas y agentes de investigación de todos los tamaños y provenientes de todos los Estados miembros de la UE. Los programas precursores del FED ya han financiado proyectos de defensa contra los drones como parte de la investigación y el desarrollo en materia de defensa.

El programa de trabajo del FED para 2023 contiene una acción para el desarrollo de la defensa contra los drones[31], con un presupuesto indicativo de 43 millones EUR. La acción tiene por objeto desarrollar módulos de *hardware* o *software* para una solución móvil global que permita hacer frente a una gran variedad de drones, incluidos los enjambres.

El principal resultado previsto del apoyo del FED en el ámbito de los drones para el período 2021-2027 es el desarrollo de un prototipo de solución de defensa contra los drones que conduzca a una posible futura adquisición conjunta a escala de la UE. Los retos tecnológicos en el ámbito de los sistemas de defensa contra los drones se abordan a través del Plan de Innovación de la UE en materia de Defensa (EUDIS). Además, el EUDIS incluye un capítulo para viveros de productos de doble uso para promover una mejor colaboración entre los ámbitos civil y de defensa y estimular la maduración tecnológica y la adaptación.

Otro pilar clave para la innovación, y específicamente para la investigación aplicada sobre cómo hacer frente a las amenazas que plantean los drones, es el trabajo del JRC. Como parte del proyecto Drone C-UAS del JRC, este revisará las tecnologías de medidas de respuesta activas y pasivas y la manera en que estas tecnologías pueden utilizarse para garantizar la seguridad de los espacios públicos y las infraestructuras críticas.

A tal fin, y como primer paso, el JRC creará un **laboratorio viviente** para estudiar las tecnologías de defensa contra los drones y cómo pueden aplicarse estas tecnologías en entornos reales. La configuración del laboratorio abarcará la planificación, preparación y aplicación de una solución. También abarcará la detección, el seguimiento, la identificación, la neutralización y la integración de las partes interesadas y los procesos. El ámbito de aplicación del laboratorio viviente incluirá la integración con sistemas de gestión del tráfico de aeronaves tripuladas y no tripuladas, en particular «U-Space»[32]. El laboratorio viviente también estudiará cómo pueden integrarse el aprendizaje automático y la inteligencia artificial para mejorar el rendimiento general de una solución de defensa contra drones.

---

[30] SWD(2022) 362 de 10 de noviembre de 2022. Tal como se describe en el informe de situación sobre la aplicación del plan de acción sobre sinergias entre las industrias de la defensa civil y espacial en el marco de la acción 9.

[31] *C(2023) 2296 Commission Implementing Decision of 29.3.2023 on the financing of the Europe Defence Fund established by Regulation (EU) No 2021/697 of the European Parliament and the Council and the adoption of the work programme for 2023 - Part II* [«C(2023) 2296 Decisión de Ejecución de la Comisión, de 29 de marzo de 2023, relativa a la financiación del Fondo Europeo de Defensa establecido por el Reglamento (UE) 2021/697 del Parlamento Europeo y del Consejo y a la adopción del programa de trabajo para 2023 - Parte II», documento en inglés].

[32] Reglamento de Ejecución (UE) 2021/664 de la Comisión, sobre un marco regulador para el U-Space. Se ha adoptado el término «U-Space» para describir la gestión del tráfico de aeronaves no tripuladas a fin de garantizar la interacción segura con otras entidades que utilizan el mismo espacio en zonas urbanas y en cualquier otra ubicación.

A medio plazo, este laboratorio viviente del JRC se convertirá en un **centro de excelencia de defensa contra los drones.**

Acciones prioritarias para aprovechar al máximo la investigación y la innovación

- **La Comisión y los Estados miembros decidirán sobre la necesidad de nuevas soluciones de defensa contra los drones en el futuro que deberán abordar los programas europeos de investigación e innovación pertinentes, en particular Horizonte Europa.**
- **La Comisión y los Estados miembros determinarán una lista de soluciones prometedoras de defensa contra los drones y evaluarán la viabilidad de la contratación precomercial de algunas de estas soluciones.**
- **La Comisión identificará ideas, tecnologías y soluciones que se integrarán en el desarrollo de las capacidades de defensa y apoyará proyectos destinados a difundir estas ideas, tecnologías y soluciones a los sectores civiles.**
- **El JRC creará un centro de excelencia de defensa contra los drones como evolución del laboratorio viviente.**

E. Apoyo financiero

La Comisión seguirá prestando apoyo financiero a las actividades pertinentes de defensa contra los drones, principalmente a través del FSI, pero también en el marco del Instrumento de Apoyo Financiero a la Gestión de Fronteras y la Política de Visados (IGFV) y el programa Horizonte Europa (para acciones relacionadas con la investigación y la innovación).

El mecanismo temático del FSI apoyará: i) las redes policiales europeas, ii) los trabajos conexos del JRC, iii) el nuevo grupo de expertos de defensa contra los drones, y iv) la creación de una plataforma de intercambio de información. La Comisión ya está financiando proyectos para poner a prueba y validar sistemas para detectar y localizar drones que cruzan ilegalmente las fronteras exteriores de la UE. Estos proyectos se basan en los resultados de anteriores proyectos de investigación financiados por la UE[33].

En el marco del mecanismo temático del FSI, la Comisión abrirá en el primer semestre de 2024 una **convocatoria de propuestas** destinada específicamente a apoyar el despliegue de soluciones de defensa contra los drones con un alto potencial de adopción.

Se animará a los Estados miembros a aplicar la presente Comunicación y a aprovechar los resultados de la investigación financiada por la UE sobre soluciones de defensa contra los drones a través de sus programas del FSI.

[33] Algunos ejemplos son los proyectos financiados en el marco de las acciones específicas del IGFV sobre: i) innovación para las fronteras marítimas/costeras o terrestres, y ii) Frontex. Algunos proyectos financiados en el marco de la acción específica sobre innovación para las fronteras marítimas/costeras o terrestres se centran en la puesta a prueba de tecnologías innovadoras de vigilancia. También existe una acción específica para la adquisición y puesta a disposición de equipos para su despliegue por parte de las autoridades fronterizas europeas con el fin de detectar y localizar drones que cruzan las fronteras en relación con actividades ilegales o delictivas. Esta acción específica permitirá a los Estados miembros adquirir dos sistemas de defensa contra los drones. Como valor añadido de la UE, a petición de Frontex en el contexto de las negociaciones bilaterales anuales, el equipo técnico adquirido en el marco de las acciones específicas debe ponerse a disposición de Frontex durante un período de hasta cuatro meses al año, para uso en sus operaciones conjuntas.

Acciones clave para el apoyo financiero

- **La Comisión pondrá en marcha una convocatoria de propuestas sobre soluciones de defensa contra los drones en el marco de los programas de trabajo del mecanismo temático del FSI para el período 2026-2027.**
- **Se animará a los Estados miembros a que hagan pleno uso de sus programas del FSI para el período 2021-2027, con el fin de identificar y aplicar soluciones eficaces contra los drones.**

F. Exploración de las medidas reglamentarias

Aunque la UE ha regulado el uso legítimo de los drones, actualmente no existen normativas específicas de defensa contra los drones a escala de la Unión que establezcan un marco armonizado común para las autoridades, los operadores y los fabricantes de los Estados miembros. Aunque las directrices no vinculantes de la AESA que abordan los incidentes con drones en los aeropuertos (mencionadas anteriormente en la presente Comunicación) fueron acogidas favorablemente por el sector, su carácter consultivo y su alcance limitado las hacen insuficientes para mitigar la amenaza que plantean los drones no cooperativos. Dada la creciente necesidad de prevenir eficazmente el uso no autorizado de drones, la Comisión, en estrecha colaboración con expertos de los Estados miembros, seguirá analizando la necesidad de desarrollar medidas legislativas o no legislativas en el futuro. A tal fin, la Comisión pondrá en marcha un **estudio analítico** específico para determinar el panorama normativo actual. Este estudio analítico también debe tener en cuenta el marco y los avances de la OACI, así como considerar que las normas para contrarrestar las amenazas potenciales que plantean los drones no deben obstaculizar indebidamente las operaciones legítimas, incluidas las actividades de pilotos de ocio organizado.

Los aeropuertos de la UE cuentan con normas de seguridad detalladas y exhaustivas que también abarcan la amenaza de los drones. Para garantizar que las autoridades de aviación y los aeropuertos sean más resilientes cuando se enfrenten a los riesgos que plantean los drones, y en consonancia con un enfoque basado en datos contrastados, la Comisión, en cooperación con los Estados miembros, **determinará otras posibles vulnerabilidades en la protección contra los drones no cooperativos en una evaluación de riesgos para la seguridad que podría requerir cambios normativos**.

En este contexto, es necesario un diálogo estructurado con la industria y los fabricantes de drones sobre las medidas de seguridad desde el diseño (por ejemplo, sistemas sólidos contra la suplantación, limitaciones de capacidad, puesta en común de protocolos de comunicación y actualizaciones de las bases de datos contra los drones).

Acciones clave para explorar medidas reglamentarias

- **La Comisión iniciará un estudio analítico para determinar las necesidades normativas y el potencial de armonización de las legislaciones y los procedimientos de los Estados miembros.**
- **En consonancia con un enfoque basado en datos contrastados, la Comisión llevará a cabo una evaluación de riesgos para la seguridad de la aviación en relación con los drones para determinar otras posibles vulnerabilidades de los aeropuertos, que podrían requerir cambios normativos.**
- **La Comisión entablará un diálogo estructurado con la industria sobre la necesidad y la naturaleza de posibles medidas específicas adicionales relacionadas con la seguridad de los drones.**

III. **PRÓXIMOS PASOS**

Para garantizar que los rápidos avances tecnológicos y el creciente número de drones no den lugar a un aumento incontrolado de las amenazas que plantean los drones no cooperativos, es necesario intensificar la cooperación a escala de la UE, sobre la base de la política global de la UE para la defensa contra los drones establecida en la presente Comunicación. A tal fin, las actividades actuales a escala de la UE continuarán y se completarán con el conjunto de medidas clave enumeradas en la presente Comunicación, que se aplicarán en los próximos años.

Las actividades descritas en la presente Comunicación abarcarán el período hasta 2030. A más tardar en 2027 se llevará a cabo un balance intermedio a través del grupo de expertos, mientras que está prevista una revisión completa del programa de la UE para la defensa contra los drones, a más tardar, en 2030.